

ABSTRACT

The present invention relates to an information distribution system including a distribution device (100) for broadcasting a content and a terminal device (200) for receiving the content broadcast from the distribution device (100). The distribution device (100) includes a PKI-related information acquisition instruction addition determination section (104) for determining whether or not PKI-related information stored therein has been updated, and a broadcast signal multiplex and transmission section (103) for, when the PKI-related information acquisition instruction addition determination section (104) determines that the PKI-related information has been updated, broadcasting a PKI-related information acquisition instruction for requesting the terminal device to acquire latest PKI-related information as being multiplexed to the content, together with information required for using the content. The terminal device (200) includes a PKI-related information acquisition determination request section (205) for, when receiving the PKI-related information acquisition instruction which is broadcast, requesting acquisition of the latest PKI-related information.